

METHOD FOR SENDING SECURITY PROTECTION MESSAGE IN COMMUNICATION SYSTEM

Publication number: JP10191459 (A)

Publication date: 1998-07-21

Inventor(s): LUO TIE + (LUO TIE)

Applicant(s): NOKIA MOBILE PHONES LTD + (NOKIA MOBILE PHONES LTD)

Classification:

- international: H04L9/30; H04Q7/38; H04L9/28; H04Q7/38; (IPC1-7): H04L9/30; H04Q7/38
- European: H04L9/30F

Application number: JP19970304553 19971106

Priority number(s): US19960744682 19961106

Abstract of JP 10191459 (A)

PROBLEM TO BE SOLVED: To send a security protection message by using a public encryption key. SOLUTION: A transmitter side uses an own public encryption key E_x to encrypt a message (c) and sends the encrypted message $E_x(c)$ to a receiver side. The receiver side uses an encryption key E_y of an object recipient of the message to encrypt the encrypted message $E_x(c)$ and to make a message $E_y(E_x(c))$ and sends the message $E_y(E_x(c))$ to the transmitter side. The transmitter side uses its own secret decoding key to decode the message $E_y(E_x(c))$ and to make $D_x(E_y(E_x(c)))=E_y(c)$ and sends the message $E_y(c)$ to the receiver side. When the receiver side is an object recipient of the message, the receiver side uses its

own decoding key D_y to decode the message and to make $D_y(E_y(c))=c$ and when the receiver side is not an objective recipient of the message, the receiver side sends it to the recipient and the recipient uses its own decoding key D_y to decode the message.

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-191459

(43)公開日 平成10年(1998) 7月21日

(51)Int.Cl.⁶

識別記号

F I

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 R

H 0 4 L 9/30

H 0 4 L 9/00

6 6 3 A

6 6 3 B

審査請求 未請求 請求項の数11 O L (全 10 頁)

(21)出願番号 特願平9-304553

(22)出願日 平成9年(1997)11月6日

(31)優先権主張番号 08/744682

(32)優先日 1996年11月6日

(33)優先権主張国 米国 (US)

(71)出願人 590005612

ノキア モービル フォーンズ リミティ
ド

フィンランド国, エフアイエヌ-02150

エスポー, ケイララーデンティエ 4

(72)発明者 ティエ ルオ

アメリカ合衆国, テキサス 76006, アー

リントン, サンライト ドライブ 2606

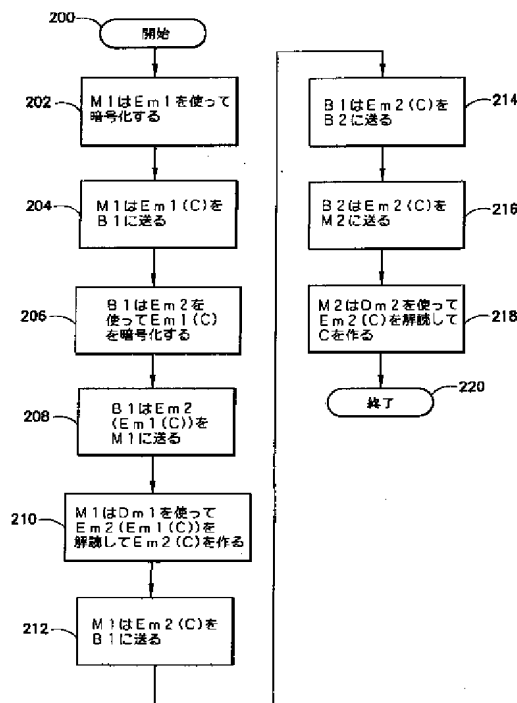
(74)代理人 弁理士 石田 敬 (外3名)

(54)【発明の名称】 通信システムにおいて機密保護メッセージを送る方法

(57)【要約】

【課題】 公開の暗号化キーを用いて機密保護メッセージを送る。

【解決手段】 送信側は自分の公開の暗号化キーExを使ってメッセージcを暗号化し、その暗号化されたメッセージEx(c)を受信側に送る。受信側は、そのメッセージの目的の受取手の暗号化キーEyを使って暗号化メッセージEx(c)を暗号化してメッセージEy(Ex(c))を作り、このメッセージEy(Ex(c))を送信側に送る。送信側は自分の秘密の解読キーを使ってそのメッセージEy(Ex(c))を解読してDx(Ey(Ex(c)))=Ey(c)を作り、このメッセージEy(c)を受信側に送る。受信側は、自分がそのメッセージの目的の受取手であるならば、自分自身の解読キーDyを使ってそのメッセージを解読してDy(Ey(c))=cを作り、自分がそのメッセージの目的の受取手ではなければ、受取手に送り、受取手が自分自身の解読キーDyを使ってそのメッセージを解読する。



【特許請求の範囲】

【請求項1】 少なくとも1つの基地局と複数の移動局とを有する通信システムで機密保護メッセージを送る方法において、前記方法は：各移動局に解読キーと公開の暗号化キーとを割り当て；第1移動局において前記第1移動局の暗号化キーを用いて第1メッセージを暗号化して第2メッセージを作り；前記第2メッセージを前記第1移動局から前記の少なくとも1つの基地局に送り；前記の少なくとも1つの基地局において第2移動局の暗号化キーを用いて前記第2メッセージを暗号化して第3メッセージを作り；前記第3メッセージを前記の少なくとも1つの基地局から前記第1移動局に送り；前記第1移動局において前記第1移動局の解読キーを用いて前記第3メッセージを解読して第4メッセージを作り；前記第4メッセージを前記第1移動局から前記の少なくとも1つの基地局に送り；前記第4メッセージを前記の少なくとも1つの基地局から前記第2移動局に送り；前記第2移動局において前記第2移動局の解読キーを用いて前記第4メッセージを解読して前記第1メッセージを作り直すステップから成ることを特徴とする方法。

【請求項2】 前記第1移動局の解読キー及び暗号化キー、並びに前記第2移動局の解読キー及び暗号化キーは、前記第2移動局の暗号化キーをメッセージに適用して第1結果を得てから前記第1移動局の解読キーをその第1結果に適用して最終結果を得ることが、前記第1移動局の解読キーを前記メッセージに適用して第2結果を得てから前記第2移動局の暗号化キーを前記第2結果に適用して前記最終結果を得ることと同等であるように構成されていることを特徴とする請求項1に記載の方法。

【請求項3】 前記第1移動局において暗号化及び解読を行う前記ステップは第1アルゴリズムに従って行われ、前記第2移動局において暗号化及び解読を行う前記ステップは第2アルゴリズムに従って行われることを特徴とする請求項1に記載の方法。

【請求項4】 前記第1アルゴリズムはRSA型のアルゴリズムから成り、前記第2アルゴリズムはラビン型のアルゴリズムから成ることを特徴とする請求項3に記載の方法。

【請求項5】 前記第1アルゴリズムはラビン型のアルゴリズムから成り、前記第2アルゴリズムはRSA型のアルゴリズムから成ることを特徴とする請求項3に記載の方法。

【請求項6】 第1及び第2の送受信装置を有する通信システムで機密保護メッセージを送る方法において、前記方法は：前記の第1及び第2の送受信装置の各々に解読キー及び公開の暗号化キーを割り当て；前記第1送受信装置において前記第1送受信装置の暗号化キーを用いて第1メッセージを暗号化して第2メッセージを作り；前記第2メッセージを前記第1送受信装置から前記第2送受信装置に送り；前記第2送受信装置において前記第

2送受信装置の暗号化キーを用いて前記第2メッセージを暗号化して第3メッセージを作り；前記第3メッセージを前記第2送受信装置から前記第1送受信装置に送り；前記第1送受信装置において前記第1送受信装置の解読キーを用いて前記第3メッセージを解読して第4メッセージを作り；前記第4メッセージを前記第1送受信装置から前記第2送受信装置に送り；前記第2送受信装置において前記第4メッセージを解読して前記第1メッセージを作り直すステップから成ることを特徴とする方法。

【請求項7】 前記第1送受信装置の解読キー及び暗号化キー、並びに前記第2送受信装置の解読キー及び暗号化キーは、前記第2送受信装置の暗号化キーをメッセージに適用して第1結果を得てから前記第1送受信装置の解読キーをその第1結果に適用して最終結果を得ることが、前記第1送受信装置の解読キーを前記メッセージに適用して第2結果を得てから前記第2送受信装置の暗号化キーを前記第2結果に適用して前記最終結果を得ることと同等であるように構成されていることを特徴とする請求項6に記載の方法。

【請求項8】 前記第1送受信装置において暗号化及び解読を行う前記ステップは第1アルゴリズムに従って行われ、前記第2送受信装置において暗号化及び解読を行う前記ステップは第2アルゴリズムに従って行われることを特徴とする請求項6に記載の方法。

【請求項9】 前記第1アルゴリズムはRSA型のアルゴリズムから成り、前記第2アルゴリズムはラビン型のアルゴリズムから成ることを特徴とする請求項8に記載の方法。

【請求項10】 前記第1アルゴリズムはラビン型のアルゴリズムから成り、前記第2アルゴリズムはRSA型のアルゴリズムから成ることを特徴とする請求項8に記載の方法。

【請求項11】 前記第2送受信装置は第1基地局から成り、前記第1送受信装置は第1移動局から成り、前記通信システムは更に第2基地局と第2移動局とを有し、前記方法は更に：前記第1メッセージを前記第1基地局から前記第2基地局に送り；前記第2基地局において前記第2基地局の解読キーを用いて前記第1メッセージを暗号化して第5メッセージを作り；前記第5メッセージを前記第2基地局から前記第2移動局に送り；前記第2移動局において前記第2移動局の暗号化キーを用いて前記第5メッセージを暗号化して第6メッセージを作り；前記第5メッセージを前記第2移動局から前記第2基地局に送り；前記第2基地局において前記第2基地局の解読キーを用いて前記第5メッセージを解読して第7メッセージを作り；前記第7メッセージを前記第2基地局から前記第2移動局に送り；前記第2移動局において前記第2移動局の解読キーを用いて前記第7メッセージを解読して前記第1メッセージを作り直すステップを有する

ことを特徴とする請求項6に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信システムのための暗号化技術に関し、特に通信システムにおいて公開の暗号化キーを使用して機密保護メッセージを送る装置及び方法に関する。

【0002】

【従来の技術】通信システム技術が進歩して、いろいろな通信システム及びサービスを利用できるようになっている。それらのシステムの中には、セルラー電話通信網、個人通信システム、種々のページングシステム、及び種々の有線及び無線のデータ通信網が含まれる。今日アメリカ合衆国で使用されているセルラー電話通信網は、AMPSアナログシステム、デジタルIS-136時分割多重(TDMA)システム、及びデジタルIS-95デジタル符号分割多重(CDMA)システムを含む。ヨーロッパでは、移動通信用広域(GSM)デジタルシステムが最も広く使用されている。これらのセルラーシステムは800-900MHzの範囲で動作する。個人通信システム(PCS)も合衆国で現在展開されている。多くのPCSシステムが1800-1900MHz範囲に対して開発されつつあるが、それらは各々主要なセルラー規格のうちの1つに基づいている。

【0003】上記の通信システムの各々において、該システムのオペレータがシステムのユーザーに機密保護通信手段を提供することが望ましいことがしばしばある。それは、該システムで動作している2つの移動局の間で機密保護メッセージを送ることを含むことがある。多くの場合にそのメッセージはテキストメッセージ等の、有限の長さのテキストメッセージである。

【0004】AMPS等のアナログシステムでは、通信内容を機密保護するのは非常に難しい。2ユーザー間で通信内容を運ぶ信号がアナログの性質であるために暗号化を簡単にも効率的にも行うことはできない。実際、標準的AMPSでは、暗号化は全く行われず、移動局と基地局との間で送られる通信メッセージは監視されたり傍受されたりされ得る。通信チャネルに使用される周波数に同調させることのできる受信装置を持っているものは誰でも、見つかることなく何時でも通信を傍受することができる。この傍受の可能性は、AMPS等のアナログシステムに結びついた1つの不都合な要素であった。この様に傍受される可能性があるために、AMPS型のシステムは機密保護メッセージを送ることを必要とする或る種のビジネスユーザーや政府筋のユーザーには好まれていない。

【0005】通信の秘密を目的として暗号化サービスを含むGSM、IS-136及びIS-95等の新しいデジタルシステムが開発されている。これらのデジタルシステムで2ユーザー間で通信メッセージを運ぶ音声信号

或いはデータ信号はデジタルの性質を持っているので、ランダム或いは疑似ランダムの性質を持っている通信信号を作るための暗号化装置を通して処理され、認可された受信装置で解読される。この様なシステムで機密保護メッセージを送りたいときには、該システムの暗号化機能を使ってメッセージを暗号化することができる。例えば、これらの規格で指定されているショートメッセージサービス(SMS)機能を使って、該システムの暗号化アルゴリズムに従って暗号化されているテキストメッセージを送ることができる。

【0006】GSM、IS-136、及びIS-95システムでは、暗号化は各ユーザーとシステムとの間のメッセージ送信に対して秘密のキー値”非公開キー”を用いて行われ、そのキーはシステムと通信するユーザーとシステムとだけに知られている。ここで検討しているPCS通信網についてのシステム規格は、特定のPCS規格の淵源となるデジタル規格、即ちGSM、IS-136、或いはIS-95において指定されている暗号化技術に基づく暗号化サービスを包含することもできる。

【0007】GSMではシステムのオペレータがシステムの各ユーザーに加入者識別モジュール(SIM)を発行することによって機密保護プロセスを制御する。SIMは、ユーザーが呼を発したり受けたりするのに使う移動局に挿入しなければならない差し込み式のチップ又はカードである。SIMは、各ユーザーに独特の、Kiと呼ばれる128ビットの数を内蔵している。このKiは、確認と、暗号化キーの導出との両方のために使われる。GSMでは、各ユーザーを確認してそのユーザーについてのKiから暗号化ビットを作成するために呼びかけと応答の手続が使われる。この呼びかけと応答の手続をホームシステムの自由裁量で実行することができる。

【0008】GSM移動局が自分のホームシステムで動作しているとき、ユーザーが自分の国際移動システム識別子/一時移動システム識別子(international mobile system identity/temporary mobile system identities (IMSI/TMSI))を呈示することによって自分が誰であるかを明らかにした後、該システムで128ビットの乱数(RAND)が作成されてその移動局のユーザーのKiと結合されて32ビットの応答(SRES)となる。このときシステムはRANDを該移動局に送り、該移動局はそのユーザーのKiから自分自身のSRES値を計算し、このRANDをシステムに送り戻す。もしその2つのSRESが調和するならば、その移動局は本物であると判断される。暗号化キー”Kc”を作るために、該移動局及び通信網の両方においてRAND及びKiを使用するアルゴリズムにより、該移動局とシステムとの間の通信のための暗号化ビットが作成される。その後、Kcは両端で機密保護通信を行うために使用される。GSM移動局が移動中であるとき、該移動局が訪れたシステムにおいて該ユーザーの登録が行われるときに、或いは

ユーザーが訪れたシステムから特別の要求が行われたときに、そのシステムにRAND、SRES及びKcの値が転送される。Ki値はホームシステム及びユーザーのSIM以外では決して使用し得ない。

【0009】IS-136及びIS-95の確認及び暗号化の処理手順は互いに同一であり、またGSMの確認及び暗号化の処理手順と似ている。IS-136システム及びIS-95システムでは、呼びかけと応答の方法も利用される。そのIS-136及びIS-95の方法は、“Aキー”と呼ばれる機密保護キーを利用する。各移動局についての64ビットのAキーはシステムのオペレータによって決定される。各移動局についてのAキーはその移動局の所有者のホームシステムとその移動局自体に記憶される。最初にAキーは米国郵便等の安全な方法で移動局の所有者に通知され得る。その所有者はキーパッドを介してそのAキーを移動局に入力することができる。或いは、Aキーを工場或いは点検修理の場所で移動局にプログラムすることもできる。Aキーは、移動局及びホームシムの両方で共有される秘密データ（shared secret data (SSD)）を所定のアルゴリズムから作成するために使われる。各移動局についてのSSDは、ホームシステムのオペレータのみが開始することのできるオーバーエア・プロトコル（an over the air protocol）の使用によってその移動局のAキーから定期的に導出され更新され得る。

【0010】IS-136及びIS-95の確認及び暗号化では、32ビットの広域呼び掛けが該移動局のサービスエリアのシステム内で所定間隔をおいて作成されて放送される。移動局がホームシステムにおいてシステム登録／呼設定アクセスを試みると、該移動局においてそのSSDから18ビットの確認応答を計算するために現在の広域呼び掛け応答が使用される。その後、その確認応答とその移動局についての呼カウント値とを含むアクセス要求メッセージが該移動局からホームシステムに送られる。そのアクセス要求を受け取ると、ホームシステムは広域呼び掛け及びその移動局のSSDを使ってそれ自身の応答値を計算する。確認応答と、その移動局のSSDと、呼カウント値を含む他の関連データとの比較によって、その移動局が本物であると確認されれば、その移動局は登録される。

【0011】移動局が訪問先のシステムでシステム登録／呼設定アクセスを試みると、現在の広域呼び掛け応答を用いて該移動局において該移動局のSSDから18ビットの確認応答を計算する。次にアクセス要求メッセージが該移動局から訪問先のシステムに送られる。訪問先のシステムでの初期登録アクセスについては、アクセス要求メッセージは移動局で計算された確認応答を含む。確認応答と広域呼び掛けとは該移動局のホームシステムに送られ、該ホームシステムはその広域呼び掛けと該移動局のSSDとを使ってそれ自身の応答値を計算す

る。確認応答同士を比較することによってその移動局が本物であると確認されたならば、その移動局のSSDと、呼カウント値を含む他の関連データとが訪問先のシステムに送られて該移動局が登録される。該移動局が関わる呼が設定されるとき、現在の確認応答値と呼カウントとが該移動局から呼設定情報とともに該システムに送られる。呼設定情報を受け取ると、訪問先のシステムは、要求をしている移動局についての記憶されているSSDと呼カウント値とを検索する。その後、訪問先のシステムは、受け取ったSSD値と現在の広域呼び掛けとが該移動局で作られたのと同じ応答を作ること確かめるために確認応答値を計算する。もしその確認応答同士と呼カウント同士とが揃うならば、その移動局は呼アクセスを許可される。通信の機密保護が希望される場合には、暗号化キー・ビットを作成するために広域呼び掛けと該移動局のSSDとを入力として用いて暗号化キーが該移動局とシステムとの両方で作成される。

【0012】GSM、IS-136及びIS-95システムで使用されるような技術についての更なる背景情報が“IEEE個人通信”の6-10頁の1995年8月付けのダン・ブラウンによる“個人通信システムにおけるプライバシー及び確認のための技術”という論文（the article “Techniques for Privacy and Authentication in Personal Communications Systems” by Dan Brown in IEEE Personal Communications, dated August 1995, at pages 6-10）に開示されている。

【0013】GSM、IS-136及びIS-95システムで使用される上記の機密キー処理手順は通信の機密を保護するものであるけれども、これらの処理手順のいずれも、傍受及び盗聴を完全に免れ得るわけではない。これらの処理手順の全てが、ユーザーのAキー又はKi値が移動局とホームシステムとの双方に知られていることを必要とする。これらの処理手順は、ユーザーのSSD又はKc値が通信リンクの両端即ちシステム及び移動局の双方において知られていることを必要とする。これらの各値がもしかすると改悪されて傍受者に知られてしまっているという可能性もあり得る。ユーザーのKi又はAキーを知っている人、或いはシステム間通信をしているユーザーのKc又はSSDを傍受した人は、機密保護されるべき通信を傍受し盗聴する可能性がある。また、各ユーザーのキーは、該ユーザーが通信をする基地局で利用可能であるので、システムの基地局を通して接続している2つの移動局が関わる暗号化通信がその基地局で破られる可能性がある。

【0014】公開キー暗号化方法は、ユーザーに公開の、即ち公然と知られ明らかにされるかも知れない暗号化キーが割り当てられるけれども、またそのユーザーにしか知られない秘密の解読キーもユーザーに割り当てられるようになっている方法である。目的の受信側ユーザーの解読キーだけがそのユーザーに宛てられた暗号化さ

れたメッセージを解読することができる、即ちその目的の受信側ユーザーの暗号化キーを使って暗号化されたメッセージを解読することができる。公開キー暗号化通信システムでは、ユーザーは解読キーを基地局やシステムから隠して自分で保管しておくことを許されるであろう。メッセージを解読するのに必要なキーを知っているのは受信側のユーザーだけであるので、公開キー暗号化方法は、例えばGSM、IS-136、或いはIS-95で使われている現在の暗号化技術で得られるよりも一層安全な通信を提供することができる。

【0015】在来の公開キー暗号化方法を使用するセルラーシステムでは、移動局Xが暗号化されたメッセージを移動局Yに送るとすると、移動局Xは、移動局Yのための公開暗号化キーと、移動局Yの暗号化キーとともに使用されなければならないアルゴリズムとの両方を知る必要がある。移動局Xが移動局Yの暗号化キーとアルゴリズムとを使ってメッセージを暗号化することができることも必要であろう。在来の公開キー暗号化方法のこれらの要件は、場合によってはセルラーシステムで使用するに当たって或る種の困難を引き起こしたり、或いは余り適していないかも知れない。

【0016】

【発明が解決しようとする課題】公開キー暗号化法を使用するに当たっての1つの難点は、暗号化と解読とに必要な計算が秘密キーシステムで必要とされるよりも遥かに多量の計算資源を必要とするかも知れないことである。移動局ではその様な計算資源には限りがあるかも知れない。二人の移動局ユーザーが各々異なる暗号化／解読アルゴリズムを使ってメッセージを秘密裏に交換したいと望む場合には資源に関する要件はもっと大きくなり得る。例えば、移動中の移動局のホームシステムのアルゴリズムとは異なる自分独自のアルゴリズムを実行するための手段をシステムオペレータが備えているシステムにその移動中の移動局が入り込んだときなどには、前記のように資源に関する要件が大きくなるかも知れない。この場合、どの移動局も、他のユーザーのアルゴリズムで暗号化を行うとともにその移動局のユーザーのアルゴリズムで解読を行うことができなければならないであろう。例えば、暗号化するために使われるアルゴリズムが、その暗号化を実行する移動局で利用し得るよりも多量の計算資源を必要とするならば、その様な要件を満たすのは困難であるかも知れない。また、特定のアルゴリズムを実行するためのコード及びデータを各移動局に記憶させておくか或いは暗号化開始前に該移動局に送信しなければならないであろうから、移動局の計算資源に対する要求が更に大きくなる。

【0017】セルラーシステムで公開キー暗号化法を使用することについてのもう一つの潜在的難点は、メッセージを送信側移動局或いは受信側移動局だけが利用し得ることを保証するために送信側の移動局が受信側移動局

の暗号化キーを知っていなければならないということである。或る種の公開キー暗号化法では暗号化キーは各々非常に大きい可能性があり、それは場合によっては数列であり、受信側となる可能性のある全ての移動局のための暗号化キーを1つの移動局に記憶させるのは困難であるかも知れない。受信側の移動局のキーがもし非常に大きければ、例えば呼設定時などに、必要に応じて送信側移動局に送ることも困難であるかも知れない。

【0018】

【課題を解決するための手段】本発明は、公開キー暗号化法を使用する通信システムにおいて機密保護メッセージを送る方法を提供する。この方法は、ユーザーの解読キーがそのユーザーの送受信装置においてのみ知られることとなるように実施される。この方法は、ユーザーの送受信装置がそのユーザーの暗号化／解読アルゴリズムと暗号化キーとを使用できるだけでよいようにも実施される。これは、特別のシーケンスを用いて2つの送受信装置間でメッセージを交換することにより実行される。この方法は、機密キー法の使用に伴う機密保護問題を回避し、各移動局がそれ自身の公開キー暗号化／解読アルゴリズムのみを実行できるようにする。この方法では、在来の公開キー暗号化法の場合のように送受信装置が目的の受信側送受信装置の暗号化キーとアルゴリズムとを使って暗号化を実行できることを必要としない。従って、送受信装置の計算資源を特定の1つのアルゴリズム向けに最適化することができる。

【0019】この方法は、各移動局或いは通信網が各々異なる暗号化／解読アルゴリズムを使用する2つの移動局間又は移動局及びセルラー通信網の間で機密保護メッセージが交換されるときに非常に安全なショートメッセージサービス(SMS)テレサービスを提供するのに役立つ。この方法は、計算量の比較的に少ない機密キーアルゴリズムを使って音声伝送などの比較的に長い通信を行えるように、通信を行う2つの移動局間で或いは移動局と通信網との間で機密キーを交換するのににも役立つ。また、1つの移動局から他の移動局又は通信網へ機密保護確認符号数(a secure authentication signature)を送るためにこの方法を使用することもできる。

【0020】本発明の或る実施例では、2つのユーザー間で交換されるメッセージのポイント間暗号化法が少なくとも1つの基地局と複数の移動局とを有する通信システムで実施される。このポイント間実施例では、該システムの基地局では解読は行われず、移動局M1のユーザーには、公然と知られる(システムに知られる)暗号化キーEm1と移動局M1においてのみ知られる解読キーDm1とが割り当てられる(“暗号化キーEmx”及び“解読キーDmx”)という用語は、ここではアルゴリズムとそのアルゴリズムで使用されるキー値との両方を指す、即ちEmxは暗号化キー値を使用する暗号化／解読アルゴリズムであり、Dmxは解読キー値を使用する

暗号化／解読アルゴリズムである)。移動局M2の他のシステムユーザーには、公然と知られる暗号化キーEm2と、移動局M2においてのみ知られる解読キーDm2とが割り当てられ、ここで $Dm1Em2 = Em2Dm1$ である。 $Dm1Em2 = Em2Dm1$ は、始めにDm1をメッセージに適用し次にEm2を適用するということは始めにEm2を次にDm1をメッセージに適用することと同じであるという制限を課すものである。M1のみがDm1を知っており、M2のみがDm2を知っている。また、M1はEm1とM1の特別の暗号化／解読アルゴリズム(A1)とを知っているだけで良く、M2はEm2とM2の特別の暗号化アルゴリズム(A2)とを知っているだけで良い。

【0021】移動局M1を持っているユーザーが移動局M2のユーザーに機密保護通信メッセージcを送りたいとき、その通信メッセージcはM1においてEm1及びA1を用いて暗号化されてメッセージEm1(c)となる。M1はこのEm1(c)をシステムの基地局B1に送る。基地局B1はEm2とA2とを用いてEm1(c)を暗号化してメッセージEm2(Em1(c))を作成し、それをM1に送り戻す。次にEm2(Em1(c))はM1においてDm1及びA1を用いて解読される。 $Dm1Em2 = Em2Dm1$ であるので、Dm1を用いてEm2(Em1(c))を解読するとEm2(c)が得られる。M1はEm2(c)をB1に送る。B1は、移動局M2が存在している区域を管理する基地局B2にEm2(c)を送る。次にEm2(c)は移動局M2に送られて移動局M2によってDm2及びA2で解読されて、移動局M1から移動局M2に送られた通信メッセージcと成る。

【0022】本発明の他の実施例では、2つの移動局間での非ポイント間暗号化法が通信システムで実施される。移動局M1のシステムユーザーには、公然と知られる(システムに知られる)暗号化キーEm1と、移動局M1においてのみ知られる解読キーDm1とが割り当てられる。M1は暗号化／解読アルゴリズムA1を使用する。移動局M2の他のシステムユーザーには、公然と知られる暗号化キーEm2と、移動局M2においてのみ知られる解読キーDm2とが割り当てられる。M2は暗号化／解読アルゴリズムA2を使用する。また、システムの各基地局Bxには、公然と知られる暗号化キーEb xと基地局Bxのみが知る解読キーDb xとが割り当てられる。各基地局はアルゴリズムAb xに従って暗号化／解読を行う。キーは、互いに通信する基地局Bxと移動局Mxとのいずれの対についても $Dm x E b x = E b x D m x$ となるように選択される。

【0023】この実施例では、移動局M1を持っているユーザーが機密保護通信メッセージcを移動局M2のユーザーに送ることを望んでいるとき、通信メッセージcはM1でEm1及びA1を用いて暗号化されてメッセー

ジEm1(c)となる。M1はこのEm1(c)をシステムの基地局B1に送る。基地局B1はEb1及びAb1を用いてEm1(c)を暗号化してメッセージEb1(Em1(c))を作り、それをM1に送る。Eb1(Em1(c))は次にM1においてDm1及びAm1を用いて解読される。 $Dm1Eb2 = Eb2Dm1$ であるので、Dm1を用いてEb1(Em1(c))を解読するとEb1(c)が得られる。次にM1はEb1(c)をB1に送る。B1は、Db1及びAb1を用いてEb1(c)を解読してcを作り、移動局M2が位置している地域を管理する基地局B2にcを送る。次にB2とM2との間で通信メッセージcはM1とB1との間での転送について述べたのと全く同様に暗号化されるが、この場合、B2、Eb2、Db2及びAb2がM1、Em1、Dm1及びAm1に代わり、M2、Em2、Dm2及びAm2がB1、Eb1、Db1及びAb1に代わる。

【0024】以下の詳細な説明を添付図面と関連させて読めば本発明の方法を一層充分に理解できる。

【0025】

【発明の実施の形態】図1は本発明の実施例に従って構成された通信システム100のブロック図である。システム100は、基地局B1及びB2、陸線通信網142、及び移動局M1及びM2から成る。2つの基地局と2つの移動局とを包含するものとして図示されているけれども、システム100は図1に示されているより多数或いは少数の基地局或いは移動局から成っていてもよい。移動局M1及びM2は、M1又はM2のユーザーと他の移動電話との間、或いはユーザーと陸線通信網142に接続された陸線電話との間で音声通信を提供する移動電話であってもよい。移動局M1及びM2は、個人通信装置或いは無線モデムを通して動作するラップトップ型コンピュータなどの、システム100についてのシステム規格に従って動作することのできる他の随他の種類の移動通信装置であってもよい。陸線通信網142は、公衆交換電話回線網(PSTN)、或いは、呼経路選択、登録、及びシステム100内での移動局の1つの基地局から他の基地局へのハンドオフを制御するための移動交換センターを包含するシステム100のための私設陸線通信網であってもよい。システム100では、移動局M1及びM2はRFリンクを通してシステム100の基地局と通信しながらシステム100の通達範囲の中を動き回ることができる。図1では、移動局M1及びM2は、それぞれRFリンク144及び146を介して基地局B1及びB2とそれぞれ通信しているものとして示されている。システム100は、RFリンクを介して移動局M1及びM2と基地局B1及びB2との間にデジタルインターフェースを提供する如何なる通信システム規格に従って動作してもよい。デジタル通信システムの設計及び動作は公知であるので、ここでは詳しくは説明しな

い。システム100はいろいろな方法で具体化され得る。例えば、システム100のデジタルRFインターフェースは、通信産業協会／電子産業協会（Telecommunications Industry Association/Electronic Industry Association (TIE/EIA)）のIS-136、IS-95、及びPCS1900規格或いはGSM規格に類似する規格に従って動作することができる。

【0026】移動局M1は、システム100の基地局と無線信号をやりとりするためのアンテナ102に結合されたトランシーバ・ユニット104を包含している。移動局M1はユーザーインターフェース108を包含しているが、それはコンピュータ・キーボードであるか、或いはキーパッド、マイクロホン及び受話口の付いている移動電話の送受器であり得る。移動局M1の制御ユニット106は、RFチャネル選択及びその他のシステム機能を通常の方法で制御し、論理ユニット112は該移動局の全般的動作を制御する。通信の機密保護を行うために使われる暗号化及び解読の機能を実現し実行するためにも論理ユニット112を利用することができる。ディスプレイ110は、移動局M1のユーザーに総合的視覚インターフェースを提供するものであり、論理ユニット112により制御される。移動局M2はトランシーバ・ユニット116、ユーザーインターフェース120、制御ユニット118、論理ユニット124、及びディスプレイ122を包含しており、これらは各々移動局M1の対応するセクションについて記載したのと同じ機能を持っている。

【0027】基地局B1は移動局と無線信号をやりとりするためのアンテナ134に結合されたトランシーバ・ユニット136を包含している。B1は制御ユニット138及び処理装置140も包含している。制御ユニット138は、移動局への適当な制御メッセージを作成することによってRFチャネル選択及び割り当てを制御するとともに、陸線通信網142とのインターフェーシングなどの他の所要のシステム機能も制御する。通信の機密保護のために使われる暗号化及び解読の機能を実現し実行するために処理装置140を利用することができる。基地局B2はトランシーバ・ユニット128、アンテナ126、制御ユニット130及び処理装置132を包含しており、これらは各々基地局B1の対応するセクションについて説明した機能を持っている。

【0028】本発明の1つの実施例では、暗号化されたメッセージをシステム100において途中で解読されることなく1つのユーザーから他のユーザーに渡すことができる。2移動局間、基地局及び移動局の間、及び、移動局と適宜の装備を持った陸線加入者局との間を含む、システム内の随意の2ポイント間でのポイント間通信を提供するためにこの実施例を使用することができる。

【0029】ポイント間メッセージ伝送を安全に行うために、システム100の各移動局Mxに、公然と知られ

る暗号化キーEmxと移動局Mxにおいてのみ知られる解読キーDmxとが割り当てられる。通信を希望している任意の2移動局M1及びM2について、Dm1Em2はEm2Dm1と等しくなければならない。しかし、M1及びM2の各々により使用される暗号化アルゴリズムは異なってもよい。MS1のユーザーがMS2のユーザーに機密保護通信メッセージcを送ることを希望しているとき、通信メッセージcはMS1においてEm1及びAm1で暗号化されて暗号化メッセージEm1(c)が作られる。MS1はこのEm1(c)をシステムの基地局B1に送る。基地局B1はEm2及びAm2を用いてEm1(c)を暗号化してメッセージEm2(Em1(c))を作り、これをMS1に送る。次にMS1はDm1及びAm1を用いてEm2(Em1(c))を解読する。Dm1Em2=Em2Dm1であるので、Dm1を用いてEm2(Em1(c))を解読するとEm2(c)が得られる。MS1はこのEm2(c)をB1に送る。B1はこのEm2(c)を、MS2が位置している地域を管理する基地局B2に送る。次にEm2(c)はMS2に送られて、MS2によってDm2及びAm2で解読されて、MS1によりMS2に送られる解読済み通信メッセージcが作られる。

【0030】ここで図2を参照すると、本発明の実施例の通信システム内でポイント間暗号化通信を行うために実行されるプロセスステップを示す流れ図が示されている。実例として、図1の移動局M1と移動局M2との間の暗号化メッセージ転送の場合を用いてこのプロセスを説明するが、M1はラビンのアルゴリズム(Rabin algorithm)を使用し、M2はライベスト、シャミル及びエイドルマン(RSA)のアルゴリズム(Rivest, Shamir and Adleman (RSA) algorithm)を使用する。ラビンのアルゴリズムについての予備的説明が、1995年にCRCにより刊行されたスティンソン(Stinson)の書籍「暗号法の理論と実際」("Cryptography, Theory and Practice")の143-148頁に記載されている。RSAアルゴリズムについての詳しい解説が1996年にジョン・ワイリー・アンド・サンズ(John Wiley and Sons)から刊行されたリンチ等(Lynch et al.)の書籍「デジタルマネー」("Digital Money")の76-86頁に記載されている。

【0031】移動局M1のためのキー関数Em1及びDm1をラビンの基準に従って選択することができる。ラビンのアルゴリズムでは、この例では、選択された所定の数Nを用いて2つの素数p及びqが選択され、ここで $p \times q = N$ であり、 $p = 4k_1 + 3$ であり、 $q = 4k_2 + 3$ であり、この k_1 及び k_2 は定数である。Nは公然と知られてもよいが、p及びqは秘密に保たなければならない。Em1は $Em1(c) = (c)^2 \bmod N$ と定義され、DM1は $DM1(c) = c^{1/2} \bmod N$ と定義され、このcは送信されるべきメッセージであ

る。DM1(c)を $c^{1/2}$ について解くために、解 $x_1 = \pm c^{(p+1)/4}$ 、及び $x_2 = \pm c^{(q+1)/4}$ を用いて方程式 $x^2 = c \pmod{p}$ と $x^2 = c \pmod{q}$ とを解く。2つの値a及びbが $ap + bq = 1$ となることが分かったならば、方程式 $c^{1/2} = bq x_1 + ap x_2 \pmod{N}$ によって $c^{1/2}$ を発見することができる。

【0032】移動局M2についてのキー関数Em2、Dm2をライベスト、シャミル及びエイドルマン(RSA)の基準に従って選択することができる。RSAでは2つの(大きな)素数p及びqが始めに選択され、ここで $p \times q = N$ である。この実施例では、M2のためのNはM1のために使われるNに等しい。それ故に $Dm1Em2 = Dm2Em1$ という条件を満たすのが簡単である。しかし、 $Dm1Em2 = Em2Dm1$ である限りは、Nの他の値を使ってもよい。その場合、2つの他の値a2及びb2が選択され、ここで $(a^2)(b^2) = 1 \pmod{(p-1)(q-1)}$ である。N及びa2は公開されてもよく、b2は秘密に保たなければならない。このとき、Em2及びDm2は $Em2(c) = (c)^{a^2} \pmod{N}$ 、及び $Dm2 = (c)^{b^2} \pmod{N}$ と定義される。

【0033】プロセスはステップ200から始まり、ここで暗号化プロセスがM1で開始される。ステップ202において、Em1及びAm1を用いて論理ユニット112により通信メッセージcが暗号化されて暗号化メッセージEm1(c) = $(c)^2 \pmod{N}$ が作られる。プロセスはステップ204に移行し、ここでEm1(c)はトランシーバー・ユニット104を通してM1からB1へ送信される。トランシーバー・ユニット136を通してEm1(c)を受け取った後、B1の処理装置140はステップ206でEm2及びAm2を用いてEm1(c)を暗号化して暗号化メッセージEm2(Em1(c)) = $((c)^2)^{a^2} \pmod{N}$ を作る。プロセスは次にステップ208に移り、ここでEm2(Em1(c))がB1からM1に送られる。次にステップ210において、B1からEm2(Em1(c))を受け取った後、M1の論理ユニット112は前記の様にAm2(ラビンのアルゴリズム)を用いてEm2(Em1(c))を解読する。 $(Em2(Em1(c)))^{1/2} = ((c)^2)^{a^2})^{1/2}$ である。作られたDm1(Em2(Em1(c)))は $(c)^{a^2} \pmod{N}$ 、即ち暗号化メッセージEm2(c)に等しい。

【0034】次に、ステップ212において、M1のトランシーバー・ユニット104は暗号化メッセージEm2(c)をB1に送る。次に、ステップ214において、B1の制御ユニット138は陸線通信網142を通してEm2(c)をB2の制御ユニット130に送る。このメッセージは暗号化されているので、これは安全な通信である。次にステップ216において、B2の制御ユニット130を通してEm2(c)を受け取った後、

トランシーバー・ユニット128はEm2(c)をM2に送る。ステップ218でEm2(c)はM2の処理装置132でDm2及びAm2を用いて解読されてDm2(Em2(c)) = $((c)^{a^2})^{b^2} \pmod{N}$ 、即ちDm2(Em2(c)) = cが作られる。このときM2は解読済み通信メッセージcを受け取ったことになる。

【0035】本発明の他の実施例では、システム100において1つのユーザーから他のユーザーにメッセージを転送するために非ポイント間法が使用される。この実施例では、送信側ユーザーと通信している基地局でそのメッセージが解読される。その後、そのメッセージは該メッセージの受取手と通信している基地局に送られて解読されて該メッセージの受取手に送られる。この実施例では、通信を行っている移動局或いは基地局の各々がそれ自身の暗号化キーと暗号化/解読アルゴリズムとを知っているだけで良い。通信を行っているエンティティは、通信を行っている他のいずれのエンティティの暗号化アルゴリズムを知らなくてもよいし、またそれを実行できなくてもよい。

【0036】一般に、この実施例では、各移動局Mxに暗号化キーEmxと解読キーDmxとが割り当てられる。Dmxは移動局xにおいてのみ知られる。システム100の各基地局Bxには暗号化キーEbxと解読キーDbxとが割り当てられる。Dbxは基地局Bxにおいてのみ知られる。互いに通信することを望んでいる移動局Mx及び基地局Byの任意の対について、DmxEbyはEbyDmxに等しくなければならない。

【0037】M1のユーザーが機密保護通信メッセージcをM2のユーザーに送ることを望んでいるとき、通信メッセージcはM1によりEm1及びAm1を用いて暗号化されてメッセージEm1(c)が作られる。M1はこのEm1(c)をシステムの基地局Bに送る。その後、基地局B1はEb1及びAb1を用いてEm1(c)を暗号化してメッセージEb1(Em1(c))を作り、これをM1に送る。次にM1はDm1及びA1を用いてEb1(Em1(c))を解読する。Dm1Eb1 = Db1Em1であるので、Dm1及びA2を用いてEb1(Em1(c))を解読するとEb1(c)が得られる。M1はこのEb1(c)をB1に送る。M1はこの時点でB1に正しいEb1(c)を送る唯一のユーザーであり得る。B1はDb1及びAb1を用いてEb1(c)を解読してcを作る。次にB1は、システムを通して、ユーザーM2が位置している地域を管理する基地局B2にcを送る。次にB2とM2との間で通信メッセージcはM1とB1との間での転送について述べたのと全く同様に暗号化され得るが、この場合、B2、Eb2、Db2及びAb2がM1、Em1、Dm1及びAm1に代わり、M2、Em2、Dm2及びAm2がB1、Eb1、Db1及びAb1に代わる。

【0038】図3を参照すると、本発明の実施例の通信

システム内で非ポイント間暗号化通信を提供するために行われるプロセスステップを示す流れ図が示されている。図3の流れ図を使って、図1の移動局M1と移動局M2との間での暗号化メッセージ転送の場合を説明することができる。この例では、M1及びM2はラビンのアルゴリズムを使用し、B1及びB2はRSAアルゴリズムを使用する。図3で使用されるプロセスでは、M1及びM2は基地局で使用されるRSAアルゴリズムを使用しなくてもよい。

【0039】移動局Myのキー関数Emy、Dmyはラビンの基準に従って選択され得る。この例についてのラビンのアルゴリズムでは、選択された数Nを用いて2つの素数p及びqが選択され、ここで $p \times q = N$ であり、 $p = 4k_1 + 3$ であり、 $q = 4k_2 + 3$ であり、 k_1 及び k_2 は定数である。Nは公然と知られてもよく、p及びqは秘密に保たなければならない。Emyは $E_{m1}(c) = (c)^2 \bmod N$ と定義され、Dmyは $D_{m1}(c) = c^{1/2} \bmod N$ と定義される。Dmy(c)をcについて解くために、解 $x_1 = \pm c^{(p+1)/4}$ 、及び、 $x_2 = \pm c^{(q+1)/4}$ を用いて方程式 $x^2 = c \bmod p$ 、及び、 $x^2 = c \bmod q$ を解く。2つの値a及びbが $ap + bq = 1$ であることが分かったならば、方程式 $c^{1/2} = bqx_1 + apx_2 \bmod N$ によりcを見いだすことができる。

【0040】基地局xについてのキー関数Ebx及びDbxをライベスト、シャミル及びエイドルマン(RSA)の基準に従って選択することができる。RSAでは、始めに2つの(大きな)素数p及びqが選択され、ここで $p \times q = N$ である。次に他の2つの値ax及びbxが選択され、ここで $(ax)(bx) = 1 \bmod (p-1)(q-1)$ である。Ebx及びDbxは、 $E_{bx}(c) = (c)^{ax} \bmod N$ 、 $D_{bx}(c) = (c)^{bx} \bmod N$ と定義される。この実施例では、B1についてのNはM1に使用されるNに等しく、B2についてのNはM2に使用されるNに等しい。それ故に、 $D_{m1}E_{b1} = E_{b1}D_{m1}$ という条件を満たすのが容易になる。しかし、 $D_{m1}E_{b1} = E_{b1}D_{m1}$ であり、且つ $D_{m2}E_{b2} = E_{b2}D_{m2}$ である限りは、Nの他の値を使用してもよい。

【0041】プロセスはステップ300から始まり、ここで暗号化プロセスが開始される。次にステップ302で、通信メッセージcはM1の論理ユニット112でEm1及びAm1を用いて暗号化され、暗号化メッセージ $E_{m1}(c) = (c)^2 \bmod N$ が作られる。次にステップ304に移行し、ここでEm1(c)はトランシーバー・ユニット104を通してM1からB1に送られる。ステップ306で、トランシーバー・ユニット136を通してEm1(c)を受け取った後、B1はEb1及びAb1を用いてEm1(c)を暗号化して、暗号化メッセージ $E_{b1}(E_{m1}(c)) = ((c)^2)^{a1}$

$\bmod N$ を作る。プロセスは次にステップ308に移行し、ここでEm2(Em1(c))はトランシーバー・ユニット136を通してM1からB1に送られる。次に、ステップ310において、トランシーバー・ユニット104を通してB1からEm2(Em1(c))を受け取った後、前述したようにM1の論理ユニット112はDm1及びラビンのアルゴリズムを用いてEb2(Em1(c))を解読する。 $E_{b2}(E_{m1}(c))^{1/2} = (((c)^2)^{a2})^{1/2}$ 。作られたメッセージDm1(Eb2(Em1(c)))は $(c)^{a2} \bmod N$ 、即ち暗号化メッセージEb2(c)に等しい。

【0042】次に、ステップ312において、M1はトランシーバー・ユニット104を通して暗号化メッセージEb1(c)をB1に送り、ステップ314においてB1の処理装置140はDb1を用いてEb1(c)を解読してDb1(Eb1(c)) = $((c)^{a1})^{b1} \bmod N = c$ を作る。処理装置140で通信メッセージcが解読された後、プロセスはステップ316に移行し、ここで通信メッセージcは基地局B1の制御ユニット138から陸線通信網142を通して基地局B2の制御ユニット130に送られる。B2とM2の間での通信メッセージcの伝送は、M1及びB1の間での転送について述べたのと全く同様に行われ得る。それはステップ318-330で説明されており、それらはステップ302-314と同一であり、B2、Eb2、Db2及びAb2がM1、Em1、Dm1及びAm1に代わり、M2、Em2、Dm2及びAm2がB1、Eb1、Db1及びAb1に代わる。

【0043】本発明の教示内容は前記の通信規格での使用のみに限定されると解されてはならず、類似の如何なるシステムをも包含すると解されるべきである。更に、上で明示的に開示した暗号化アルゴリズム以外の暗号化アルゴリズムを使用して本発明を実施してもよい。

【0044】本発明は、その好ましい実施例に関して具体的に図示され解説されており、本発明の範囲から逸脱することなく形及び細部に変更を加え得ることが当業者に理解されるであろう。

【図面の簡単な説明】

【図1】本発明の実施例に従って構成された通信システムのブロック図である。

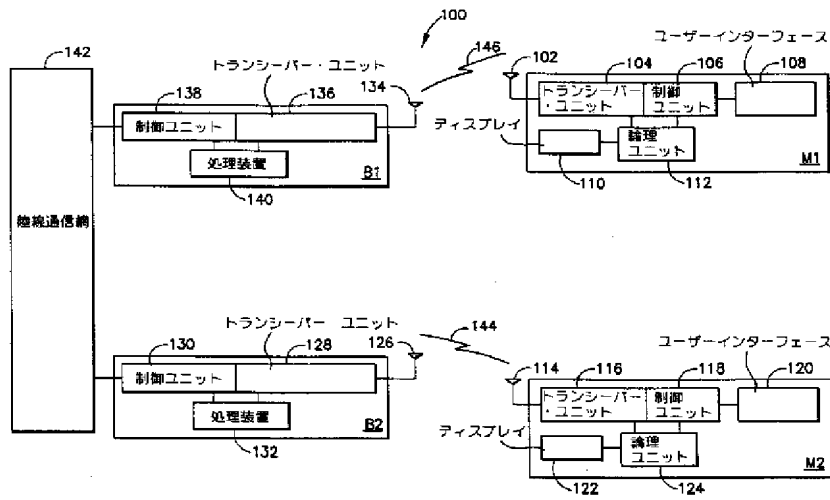
【図2】本発明の実施例の通信システム内でポイント間暗号化通信メッセージを提供するために行われるプロセスステップを示す流れ図である。

【図3】本発明の実施例の通信システム内で非ポイント間暗号化通信メッセージを提供するために行われるプロセスステップを示す流れ図である。

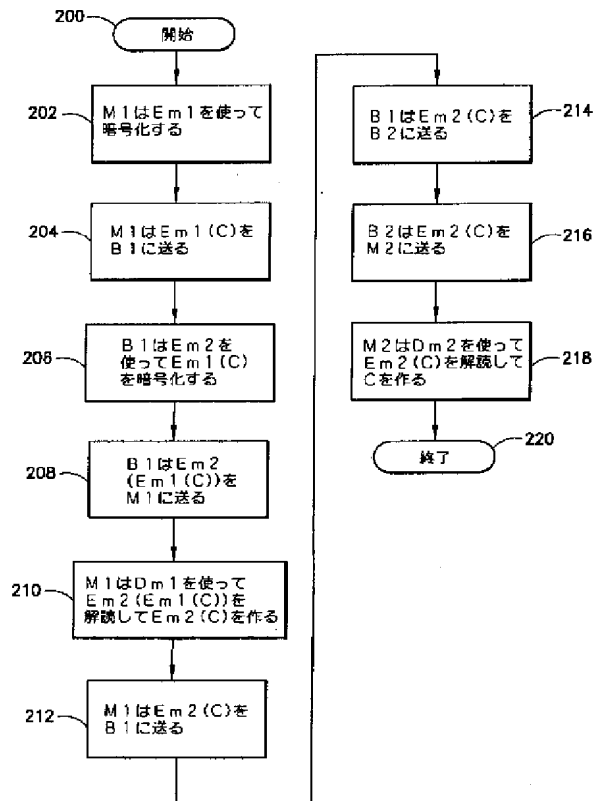
【符号の説明】

B1、B2…基地局
M1、M2…移動局

【図1】



【図2】



【図3】

